# Derivative Classification Training

## Derivative Classification

Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or documents, or a classification guide issued by an Original Classification Authority (OCA).

While working with classified information, individuals sometimes generate or create new documents and materials based upon that classified information. Individuals who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. The newly created documents must be classified based upon the classification level of the information from which the new document was developed. This is Derivative Classification.

# Derivative Classification Training

## Original Classification Authority (OCA)

An OCA is an individual occupying a position designated in writing that is charged with making the initial determination that information requires protection against unauthorized disclosure in the interest of national security. When applying derivative classification to documents generated from classified information, Derivative Classifiers must observe and respect the classification determination of the Original Classification Authority (OCA).

## Derivative Classifiers

The individuals responsible for applying derivative classification to documents are called Derivative Classifiers. Derivative Classifiers are responsible for maintaining the protection and integrity of classified information. These individuals must possess expertise regarding the subject matter of the classified information, as well as classification management and marking techniques. When applying derivative classification to documents generated from classified information, Derivative Classifiers must observe and respect the classification determination of the Original Classification Authority (OCA).

## Training Requirements

- To accurately apply derivative classification, individuals must only use authorized sources.
- Prior to applying derivative classification markings, personnel must be trained in proper application of derivative classification principles.
- Derivative Classifiers who do not receive training at least once every 2 years, shall not be authorized or allowed to derivatively classify information until they have received training.

# Derivative Classification Training

## Principles of Derivative Classification

The principles of derivative classification are:

- Use only authorized sources for classification guidance. The use of only memory or “general rules” about the classification of broad classes of information is prohibited.
- Observe and respect the classification determinations made by the OCA.
- Identify yourself by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action.
- Apply standard markings to the derivatively classified material.
- Take appropriate and reasonable steps to resolve doubt or conflict about classification, level of classification, and duration of classification of information.
- Use caution when paraphrasing or restating information.
- Avoid unnecessary classification or over-classification of information.

## Authorized Sources

As stated in the Principles, individuals should only use authorized sources of classification guidance.  These are:

- Security classification guides
- Properly marked source documents
- Department of Defense (DD) Form 254

## Prohibitions and Limitations

In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

- Conceal violations of law, inefficiency, or administrative error;
- Prevent or delay the release of information that does not require protection in the interest of national security;
- Prevent embarrassment to a person, organization, or agency; or
- Restrain competition.

## Classification Duration

The duration specified on derivative documents must respect the duration specified by the OCA. The most restrictive declassification instruction (the one that specifies the longest duration of classification) must be carried forward.  If the source document or applicable security classification guide provides no declassification instruction from the OCA, or obsolete or invalid declassification instructions are specified, Derivative Classifiers should apply a calculated 25-year duration from the date of the source document.

Examples of classification duration include:

- A date or event 10 years from origination.
- A date or event up to 25 years.
- 25X1 through 25X9, with a date or event.
- 50X1–HUM or 50X2–WMD, or Information Security Oversight Office (ISOO)-approved designator reflecting the Interagency Security Classification Appeals Panel (ISCAP) approval for classification beyond 50 years.

## Multiple Sources

When derivatively classifying documents from multiple sources, the date or event for declassification that corresponds to the longest period of classification, from either the SCG or source document, shall be carried forward for derivative classification. When material is derivatively classified based on “multiple sources” (i.e., more than one security classification guide, classified source document, or combination thereof), the derivative classifier shall compile a list of the sources used. This list shall be included in or attached to the document.

## Classification Markings

The Derivative Classifier should apply the following guidelines for classification markings:

- Classification markings shall be indicated in a manner that is immediately apparent.
- Each portion of a derivatively classified document shall be marked immediately preceding the portion to which it applies.
- Information must be marked as one of the three classification levels defined in E.O. 13526 (Top Secret, Secret, or Confidential).
- The “Classified By” line must include the name and position, or personal identifier, of the Derivative Classifier.
- All classified documents should include date of origin, agency and office or origin.
- Declassification instructions must be included on the document.
- Classified addenda or unclassified versions of documents should be used whenever practicable to facilitate greater information sharing.

**Derivative Classifier Identification:** Individuals who derivatively classify must be identified by name and position, or by personal identifier in a manner that is immediately apparent for each classification action. This information must be included in the “Classified By” line. Also, identify the agency and office of origin, if not otherwise evident.

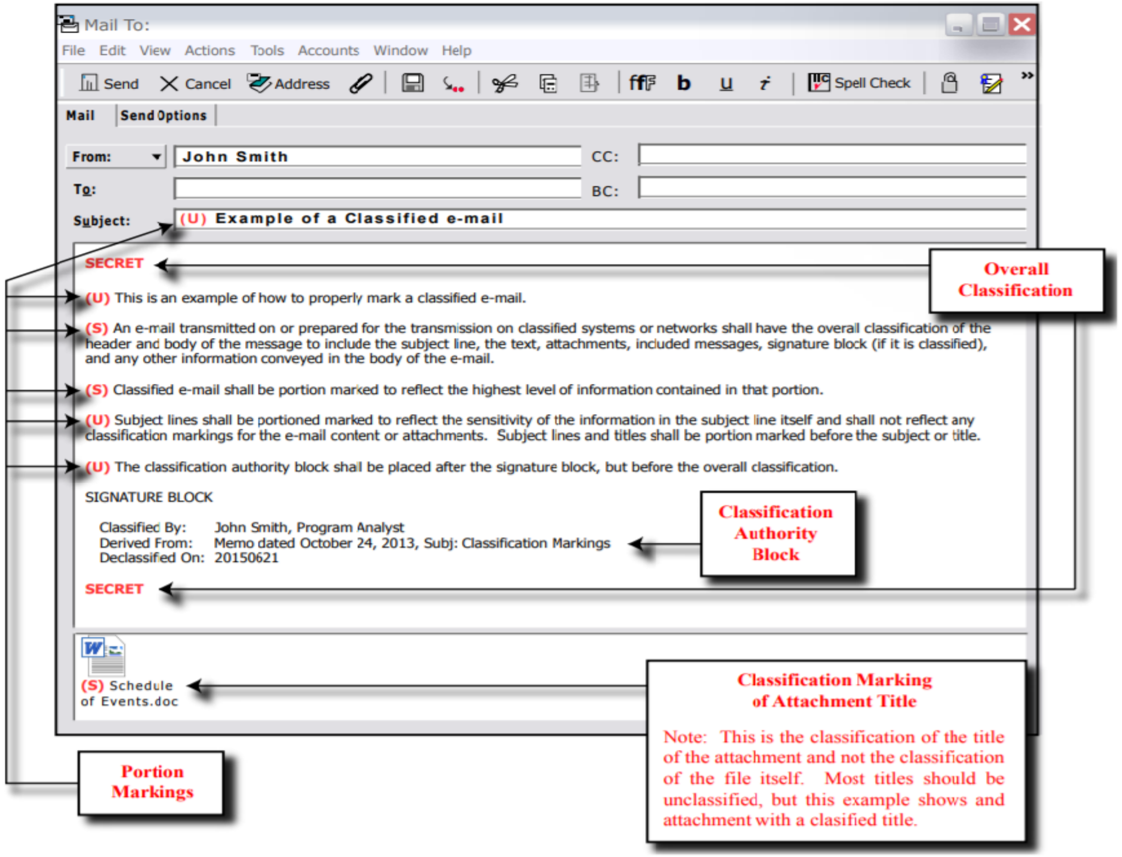
**Banner Markings:** The derivative document must be conspicuously marked at the top and bottom with the highest classification level of information found in any portion of the document. If the derivative document contains more than one page, each page will be marked with an overall marking.

**Portion Marking:** When using more than one classified source document in creating a derivative document, portion mark the classified information incorporated in the derivative document with the classification level indicated on the source documents. For example, if paragraph one of the derivative document incorporates “Secret” information from paragraph one of Source 1, and paragraph two of the derivative document incorporates “Confidential” information from paragraph one of Source 2, each should be marked accordingly.

**Compilation:** Compilation is combining or associating individual pieces of unclassified information to reveal information that, together, is classified. Derivative Classifiers must explain classification by compilation on the face of the document.

# Derivative Classification Training

## Examples of Classification Markings



From: John Smith

CC:

To:

BC:

Subject: (U) Example of a Classified e-mail

SECRET

(U) This is an example of how to properly mark a classified e-mail.

(S) An e-mail transmitted on or prepared for the transmission on classified systems or networks shall have the overall classification of the header and body of the message to include the subject line, the text, attachments, included messages, signature block (if it is classified), and any other information conveyed in the body of the e-mail.

(S) Classified e-mail shall be portion marked to reflect the highest level of information contained in that portion.

(U) Subject lines shall be portioned marked to reflect the sensitivity of the information in the subject line itself and shall not reflect any classification markings for the e-mail content or attachments. Subject lines and titles shall be portion marked before the subject or title.

(U) The classification authority block shall be placed after the signature block, but before the overall classification.

SIGNATURE BLOCK

Classified By: John Smith, Program Analyst
Derived From: Memo dated October 24, 2013, Subj: Classification Markings
Declassified On: 20150621

SECRET

(S) Schedule of Events.doc

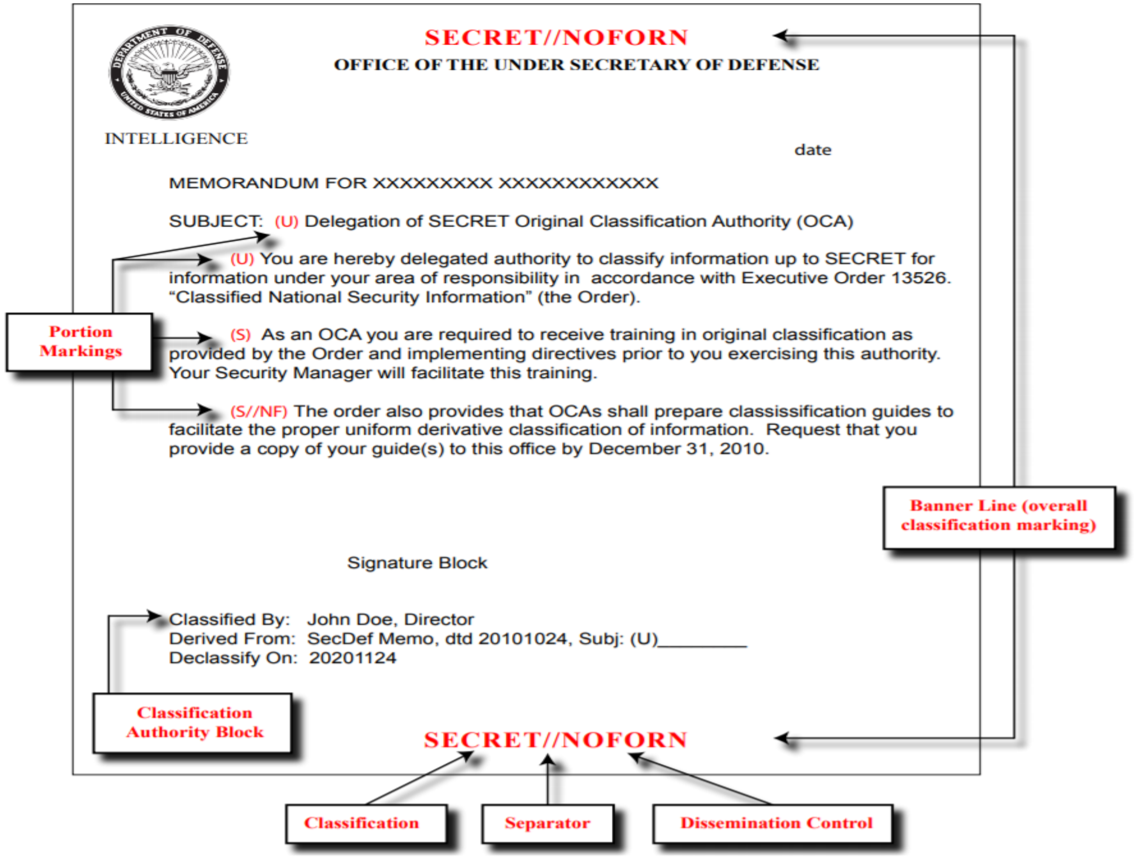
Overall Classification

Classification Authority Block

Classification Marking of Attachment Title

Note: This is the classification of the title of the attachment and not the classification of the file itself. Most titles should be unclassified, but this example shows and attachment with a clasified title.

Portion Markings



SECRET//NOFORN

OFFICE OF THE UNDER SECRETARY OF DEFENSE

INTELLIGENCE

date

MEMORANDUM FOR XXXXXXXXX XXXXXXXXXXXX

SUBJECT: (U) Delegation of SECRET Original Classification Authority (OCA)

(U) You are hereby delegated authority to classify information up to SECRET for information under your area of responsibility in accordance with Executive Order 13526. “Classified National Security Information” (the Order).

(S) As an OCA you are required to receive training in original classification as provided by the Order and implementing directives prior to you exercising this authority. Your Security Manager will facilitate this training.

(S//NF) The order also provides that OCAs shall prepare classissification guides to facilitate the proper uniform derivative classification of information. Request that you provide a copy of your guide(s) to this office by December 31, 2010.

Signature Block

Classified By: John Doe, Director
Derived From: SecDef Memo, dtd 20101024, Subj: (U)________
Declassify On: 20201124

SECRET//NOFORN

Portion Markings

Banner Line (overall classification marking)

Classification Authority Block

Classification

Separator

Dissemination Control

# Derivative Classification Training

## Sources of Classification Guidance

A Security Classification Guide (SCG) is a collection of precise, comprehensive guidance about a specific program, system, operation, or weapons system identifying what elements of information are classified. For each element of information, the SCG includes its classification level, the reason(s) for that classification, and information about when that classification will be downgraded or declassified.

For this reason, SCGs are the primary source guide for derivative classification.

### Source Documents

A second authorized source for derivative classification is an existing, properly marked source document from which information is extracted, paraphrased, restated, and/or generated in a new form for inclusion in another document. If there is an apparent marking conflict between a source document and an SCG regarding a specific item of information, derivative classifiers must follow the instructions in the SCG.
A list of source material carried forward from the source document must be included in or attached to the new document.

### DD Form 254 (for Contractors)

The third authorized source is the DD Form 254, the Department of Defense Contract Security Classification Specification. The DD Form 254 provides classification guidance to contractors performing on classified contracts. The form identifies the level of information they will need to access, the required level of security clearance for access, and the performance requirements. For example, performance requirements may include safeguarding and special security requirements. The DD Form 254 commonly refers the reader to another document such as an SCG for specific classification guidance.

## Declassification Instructions

Classified documentation is reviewed periodically to determine if the information should be declassified. The date of declassification and duration between reviews is defined in the declassification instructions. The following guidelines are applicable to declassification instructions:

- When declassification dates are displayed numerically, the following format shall be used: YYYYMMDD.
- The date of origin of source documents must also be included with declassification instructions.

### “Declassify on” Line

Specify the date or event for declassification, exemption category with date or event for declassification, or other declassification instruction corresponding to the longest period of classification among the source document(s), security classification guide(s), and other applicable classification guidance issued by the OCA.  If the document is classified by “Multiple Sources” and different declassification instructions apply to information included, determine the MOST RESTRICTIVE declassification instruction that applies to any of the source information and place it on the “Declassify on” line. This will ensure all the information in the document is protected for as long as necessary.

### Obsolete Declassification Instructions

When a document is classified derivatively, either from a source document(s) or a classification guide, that contains one of the following obsolete declassification instructions, ‘‘Originating Agency’s Determination Required’’ or ‘‘OADR,’’ “Manual Review” or “MR,” or any of the exemption markings “X1, X2, X3, X4, X5, X6, X7, and X8,” the derivative classifier shall calculate a date that is 25 years from the date of the source document when determining a derivative document’s date or event to be placed in the “Declassify on” line.  If no source date is available, then use the current date.

**Classification Level Review:** Classified documentation is reviewed periodically to determine if the level of classification should be maintained, upgraded, downgraded, or declassified.

# Derivative Classification Training

## Classification Challenges

Authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information they believe is improperly classified.  A challenge to a classification decision occurs when the holder of information has substantial cause to believe that the information has been improperly or unnecessarily classified.

Informal questioning of classification is encouraged before resorting to formal challenge. If the authorized holder has reason to believe the classification applied to information is inappropriate, he or she should contact the classifier of the source document or material to address the issue. Additional information regarding classification challenges is available through STEPP course: Classification Conflicts and Evaluations IF110.16

## Sanctions and Management Actions

We are subject to the DoD established procedures to ensure that prompt and appropriate management action is taken in case of compromise of classified information, improper classification of information, and incidents that may put classified information at risk of compromise.

Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.  Guidance from the DoD states that management actions should focus upon correction or elimination of the conditions that caused or occasioned the incident.

Individuals shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

- Disclose properly classified information to unauthorized persons;
- Classify or continue the classification of information in violation of the order;
- Create or continue a special access program contrary to the requirements of this order; or
- Contravene any other provision of E.O. 13526 or its implementing directives.